Cyber-Attacken mit Verschlüsselungstrojanern

Zum eigenen Schutz sollten Unternehmen Prävention systematisieren und laufend aktuell halten

Ein Cyber-Angriff kann jedes Unternehmen treffen, egal welcher Größe. Wenn Malware ins System erstmal eingedrungen ist, wird es häufig richtig teuer.

Cyberkriminelle nutzen jede noch so kleine Schwachstelle aus, sei sie technischer oder organisatorischer Art, um Zugriff auf sensible Unternehmensdaten zu bekommen bzw. um eben diese Daten zu verschlüsseln. „Die Angriffe der jüngsten Vergangenheit auf die ODAV AG (IT-Dienstleister der Handwerkskammern), die IT-Systeme der Unfallkasse Thüringen (UKT) oder die Thyssenkrupp AG sind aktuelle Beispiele", so IHK-Referent Rico Seyd.

„Attacken mit Verschlüsselungssoftware sind für Cyberkriminelle ein lukratives Geschäftsmodell", erläutert Markus Vollmuth, Informationssicherheitsberater und ISO 27001 Lead Auditor bei der atarax Unternehmensgruppe. Opfer von Cyber-Angriffen mit Erpressungssoftware haben im vergangenen Jahr 2023 umgerechnet erstmals mehr als eine Milliarde Euro an Lösegeld bezahlt. Das geht aus dem „Crypto Crime Report 2024" der Analysefirma Chainalysis hervor.

Der Schaden, der mit „Ransomware" zusätzlich zur gezahlten Lösegeldsumme z. B. durch Produktionsausfälle oder durch Imageschäden angerichtet wird, ist allerdings noch viel höher.

„Der Begriff „Ransomware" steht für eine Art von Schadprogrammen, die den Zugriff auf Daten und Systeme durch Verschlüsselung einschränken oder unterbinden", weiß Markus Vollmuth. Für die Entschlüsselung wird dann ein Lösegeld (englisch: Ransom) verlangt.

Welche Maßnahmen können Sie im Unternehmen präventiv ergreifen, um sich vor Cyber-Angriffen zu schützen:

- Sensibilisieren Sie Ihre Mitarbeiterinnen und Mitarbeiter zu aktuellen Angriffsmethoden und zu geltenden Sicherheitsbestimmungen im Unternehmen.
- Nutzen Sie technische Maßnahmen wie Antiviren-Software, Firewalls, Netzsegmentierung etc., um Angriffe abwehren zu können.
- Halten Sie Ihre Hard- und Software auf dem aktuellen Stand. So können bekannte (technische) Sicherheitslücken nicht mehr ausgenutzt werden.
- Entwickeln Sie eine geeignete Backup-Strategie, um im Notfall verlorene oder verschlüsselte Daten wiederherstellen zu können. Das Backup bzw. dessen Wiederherstellung sollte regelmäßig getestet werden.
- Entwickeln Sie Meldewege, die die Mitarbeiter nutzen können, um einen Vorfall zu melden .
- Schaffen Sie eine IT-Notfallorganisation, die bei einem IT-Notfall (z. B. Ransomware-Angriff) tätig wird. ■

Autoren: Markus Vollmuth (Informationssicherheitsberater bei der atarax Unternehmensgruppe) und Rico Seyd (Referent IHK zu Coburg)

Information
tinyurl.com/massnahmen-cyber-angriff

IT-Schwachpunkte erkennen und schließen

Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet Unternehmen Newsletter an

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt proaktiv Unternehmen in der Abwehr von Cyberangriffen, vor allem durch Know-how-Transfer.

Die Digitalisierung in Unternehmen schreitet rasant voran und eröffnet unseren Firmen ganz neue Chancen. „Doch unzureichend geschützte Systeme bieten Cyber-Kriminellen viele Möglichkeiten, sensible Daten auszuspähen und Geräte oder Prozesse zu sabotieren", so IHK-Referent Rico Seyd. Hinzu kommt, dass ein Unternehmen alle seine potenziellen Schwachpunkte absichern muss – denn einem Angreifer genügt es, einen einzigen ausfindig zu machen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung für die Wirtschaft durch Prävention, Detektion und Reaktion. Zum Bereich der Prävention zählen zahlreiche, kostenfreie Newsletter des BSI, die interessierte Unternehmen mit aktuellen Informationen aus verschiedenen Themenbereichen versorgen: (1) BCM-Info - Business Continuity Management; (2) Cloud-Computing (derzeit inaktiv); (3) IT-Grundschutz; (4) Kleine und mittlere Unternehmen (KMU); (5) Mindeststandards Bund; (6) Verbraucherschutz-Newsletter „Sicher informiert". ■

© BSI/Bernd Lammel/bundesfoto

Seit Februar 2024 ist das Nationale IT-Lagezentrum des BSI in seinen neuen Räumlichkeiten in Betrieb. Die Arbeitsplätze im Lagezentrum wurden verdoppelt und die neueste Medientechnik verbaut, um im 24/7 Informationsdauerdienst die Cybersicherheitslage Deutschlands zu jeder Tages- und Nachtzeit bewerten zu können.

Information
tinyurl.com/bsi-newsletter